REMARKS

The Office Action dated February 24, 2006 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 13, 15, 16, and 20 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 14 and 23 have been canceled without prejudice or disclaimer. No new matter has been added. Therefore, claims 1-4, 7-9, 12-13, 15-17, 19-22, and 27-29 are currently pending in the application.

The Office Action indicated that claims 1-4, 7-9, and 12 have been allowed. Applicants thank the Examiner for the allowance of these claims. Claims 13, 15-17, 19-22, and 27-29 are respectfully submitted for consideration.

Claims 13-17, 19-23, and 27-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all of the elements of the claims, with the exception of acquiring the guess passcode from a manufacturer. The Office Action cites Angelo as allegedly curing this deficiency in Tello. Applicants respectfully submit that the claims recite subject matter which is neither disclosed nor suggested by the cited prior art, as will be discussed below.

Claim 13, upon which claims 15-17 and 19 are dependent, recites a component for selectively enabling functionality of an electronic device. The component includes means for generating an encrypted bit string. The means for generating an encrypted bit string includes a public key encryption module, a public key module in communication with the public key encryption module, which has a public key stored therein, and a guess register in communication with the public key encryption module. The public key encryption module receives the guess passcode from the guess register and the public key from the public key module in order to generate a ciphertext bit string. The component further includes means for acquiring the guess passcode including a host in communication with the means for generating an encrypted bit string. The component also includes a hash function module in communication with an on board memory, the on board memory having a predefined identification number stored therein. The hash function module receives an identification number from the on board memory and generates a corresponding hash value therefrom. The component further includes means for determining if the ciphertext bit string matches the hash value, and means for outputting a functionality enable signal when the means for determining determines that the ciphertext bit string matches the hash value.

Claim 20, upon which claims 21-22 and 27-29 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of encrypting a first bit string and a second bit string to generate a third bit string, calculating a fourth bit string, comparing the fourth bit string to the third bit string, generating a function enable signal in accordance with the comparison, and selecting at least one of a bonding option output and the function enable signal as a final enable output. The encrypting step further includes the step of determining a guess passcode, which includes requesting the guess passcode from a manufacturer. The comparing step further includes receiving the fourth bit string representing a hash value and the third bit string representing a cipher text bit string in at least one input of a comparator, and determining if the fourth bit string matches the third bit string.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, the cited references of Tello and Angelo, whether considered alone or in combination, fail to disclose or suggest the elements of the claims, and therefore fail to provide the advantages and features discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that the combination of Tello and Angelo fail to disclose or suggest all of the elements of claims 13 and 20. For example, Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest "means for determining if the ciphertext bit string matches the hash value; and means for outputting a functionality enable signal when the means for determining determines that the ciphertext bit string matches the hash value," as recited in claim 13. Similarly, Tello and Angelo do not disclose or suggest that the comparing step includes "receiving the fourth bit string representing a hash value and the third bit string representing a cipher text bit string in at least one input of a comparator; and determining if the fourth bit string matches the third bit string," as recited in claim 20.

According to certain embodiments of the present invention, an identification module 28 is used to store a component identification number. The component identification number is transmitted from identification module 28 to hash function module 29. The hash function module 29 is configured to receive the pre-image input from identification module 28 and output a hash value. The hash value generated by hash function module 29 is transmitted to comparator 20 as a second input 20b. Further, host 18 obtains a guess passcode from the manufacturer and transmits the guess passcode to guess register 19. The guess passcode is then transmitted as clear text to public key encryption module 35 (Specification, page 23, lines 9-23 and Fig. 3).

Additionally, as discussed in the present specification, public key module 34, which contains the public key for the device, transmits the public key to public key encryption module 35. Therefore, public key encryption module 35 receives both the guess passcode and the public key as clear text inputs. These two inputs are processed/encrypted by public key encryption module 35 to generate cipher text at the output thereof. This cipher text is transmitted to the first input 20a of comparator 20. Comparator 20 then compares the cipher text received from the public key encryption module 35 representing the guess passcode with the hash value generated by the hash function module representing the identification number of the component. If the comparator 20 determines that these two values match, then an enable signal is output from comparator 20 indicating that the device 33 has determined that the guess passcode is authentic and that the corresponding functionality of the component should be enabled (Specification, page 24, lines 1-20 and Fig. 3).

Applicants respectfully submit that Tello and Angelo fail to disclose or suggest the above-discussed configuration, as recited in claims 13 and 20. Tello merely discloses that a software program in the flash memory of the security engine compares a hash number in the smart card with a hash number in the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed (Tello, Column 5, lines 21-35). Tello does not disclose or suggest comparing a cipher text bit string generated by an encryption module with a hash value generated by a hash function module and generating a function enable output based on the comparison. Specifically, Tello fails to disclose "means for determining if the ciphertext bit string matches the hash value; and means for outputting a functionality enable signal when the means for determining determines that the ciphertext bit string matches the hash value," as recited in claim 13, and "receiving the fourth bit string representing a hash value and the third bit string representing a cipher text bit string in at least one input of a comparator; and determining if the fourth bit string matches the third bit string," as recited in claim 20. Although Tello discloses that hash numbers are created from personal information stored in the Identification area (Tello, Column 16, lines 31-34), Tello makes no mention of comparing the hash numbers with a cipher text bit string generated by an encryption module in order to generate a function enable output for the component. Angelo also fails to disclose or suggest these limitations of the claims.

Therefore, the combination of Tello and Angelo fails to disclose or suggest comparing a ciphertext bit string generated by the encryption module with a hash value generated by the hash function module to generate an enable output for the component, as recited in the claims. As such, Applicants respectfully request that the rejection of claims 13 and 20 be withdrawn.

Claims 15-17, 19, 21-22, and 27-29 are dependent upon claims 13 and 20, respectively. Accordingly, claims 15-17, 19, 21-22, and 27-29 should be allowed for at least their dependence upon claims 13 and 20, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-4, 7-9, 12-13, 15-17, 19-22, and 27-29 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf